

Cyberbezpieczeństwo

W trosce o bezpieczeństwo mieszkańców publikujemy podstawowe informacje dotyczące zagrożeń związanych z cyberbezpieczeństwem oraz zasad bezpiecznego korzystania z internetu, poczty elektronicznej i urządzeń mobilnych.

Cyberzagrożenia mogą dotknąć każdego użytkownika internetu – zarówno podczas korzystania z bankowości elektronicznej, portali społecznościowych, zakupów online, jak i codziennej komunikacji e-mailowej.

Najczęstsze zagrożenia w sieci

- **Phishing** – próby wyłudzenia danych poprzez podszywanie się pod banki, urzędy, firmy kurierskie lub inne zaufane instytucje.
- **Fałszywe wiadomości e-mail i SMS** – zawierające linki prowadzące do spreparowanych stron logowania lub płatności.
- **Złośliwe oprogramowanie** – wirusy, trojany i inne aplikacje mogące przejąć dane lub zakłócić działanie urządzenia.
- **Kradzież haseł** – wynikająca z używania prostych haseł albo tych samych danych logowania w wielu serwisach.
- **Oszustwa internetowe** – fałszywe sklepy, aukcje, inwestycje lub podszywanie się pod znajomych i członków rodziny.

Podstawowe środki ostrożności

- Nie klikaj w podejrzane linki przesyłane w wiadomościach e-mail, SMS lub komunikatorach.
- Nie podawaj loginów, haseł, kodów BLIK ani danych kart

płatniczych na stronach, co do których nie masz pełnej pewności.

- Zawsze sprawdzaj adres strony internetowej przed zalogowaniem się do banku lub innego ważnego serwisu.
- Stosuj silne i unikalne hasła do różnych usług.
- Włącz uwierzytelnianie dwuskładnikowe (2FA), jeśli jest dostępne.
- Regularnie aktualizuj system operacyjny, przeglądarkę internetową oraz program antywirusowy.
- Zachowuj ostrożność wobec wiadomości wywołujących presję czasu, niepokój lub obietnicę szybkiego zysku.
- Nie instaluj programów i aplikacji z nieznanym źródłem.

Na co zwrócić szczególną uwagę?

Cyberprzestępcy bardzo często wykorzystują pośpiech i nieuwagę użytkowników. Przykładowe wiadomości mogą dotyczyć:

- rzekomej niedopłaty do przesyłki,
- blokady konta bankowego,
- konieczności pilnego zalogowania się do serwisu lub urzędu,
- wyjątkowej okazji zakupowej lub inwestycyjnej,
- prośby o pilną pomoc finansową od osoby podszywającej się pod znajomego.

W przypadku jakichkolwiek wątpliwości należy przerwać działanie, nie otwierać podejrzanych linków i samodzielnie zweryfikować informację u źródła.

Przydatne portale i materiały z zakresu cyberbezpieczeństwa

Poniżej znajdują się wybrane portale zawierające artykuły,

ostrzeżenia oraz materiały edukacyjne związane z cyberbezpieczeństwem:

- www.cert.pl
- <https://cyberpolicy.nask.pl>
- <http://www.cyber.mil.pl>
- <https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo>

Dodatkowe źródła wiedzy

- [Baza wiedzy cyberbezpieczeństwa](#)
- [Narodowe Standardy Cyberbezpieczeństwa](#)

Zachęcamy do regularnego śledzenia komunikatów i porad publikowanych przez wiarygodne instytucje zajmujące się ochroną użytkowników w sieci. Wiedza i ostrożność to podstawowe elementy skutecznej ochrony przed cyberzagrożeniami.